

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

UNITED STATES OF AMERICA

v.

Case No. 1:19-CR-227

MATTHEW HASH,

Defendant.

STATEMENT OF FACTS

The United States and the defendant, MATTHEW HASH (hereinafter, "the defendant"), agree that at trial, the United States would have proven the following facts beyond a reasonable doubt with admissible and credible evidence:

1. From in and around December 2014, and continuing thereafter up to and including September 2, 2015, in the Eastern District of Virginia and elsewhere, the defendant did knowingly and unlawfully combine, conspire, confederate and agree with others, both known and unknown, to knowingly and intentionally devise a scheme and artifice to defraud Company A and its customers, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and to transmit and cause to be transmitted by means of wire communications in interstate commerce a writing, sign, signal, picture, and sound for the purpose of executing such scheme and artifice.

2. Company A is an apparel and home fashions retailer. It owns and operates stores in and outside of the United States.

3. As part of its business, Company A offers store gift cards for sale. In addition, when a customer returns store merchandise without a receipt, Company A frequently issues a gift card to the customer in the amount of the returned merchandise.

4. Each gift card that Company A issues has a unique identifying number (hereafter, “account number”). The account number is printed on the gift card itself and encoded electronically onto a black, magnetic strip on the card. When a gift card is scanned at a point of sale, the account number that is encoded on the card is charged.

5. During the period of the conspiracy, Company A contracted with a Florida-based company, Company B, to process its financial transactions that involved Company A gift cards. When customers engaged in retail transactions at Company A’s stores using gift cards to purchase or return items, electronic data from the sale or return were transmitted immediately by wire from the cash register terminals to Company B in Florida. Backup data from the transactions were then sent via wire to the Company A mainframe computer in Ohio.

6. In or around early December 2014, the defendant met Jarrod Gray, who was employed as an Internal Fraud Investigator by Company A. Until his termination on or about September 2, 2015, Gray’s duties included conducting internal fraud investigations of Company A employees in Northern Virginia and West Virginia. By virtue of his employment, Gray had access to Company A computer databases that contained internal electronic records concerning the issuance and use of Company A store gift cards, including the monetary balance and account numbers of the cards.

7. At or around the time of their meeting, Gray and the defendant entered into an agreement to participate in a scheme involving the fraudulent use of Company A gift cards. Pursuant to their agreement, the defendant provided Gray with Company A gift cards that did not have any value on them. Gray used his position at Company A to obtain account numbers for existing Company A gift cards without the cardholders’ authorization. Many of the account numbers that Gray obtained were high-value cards (i.e., they had large balances on credit). Using

a magnetic card encoder, Gray encoded the account numbers onto the magnetic strips of the cards provided by the defendant. This process of re-encoding a gift card with an account number that does not match the number printed on the card is known as “cloning.”

8. During and in furtherance of the conspiracy, the defendant recruited, managed, and directed multiple other co-conspirators to use the cloned gift cards to purchase merchandise and new, “clean” gift cards (i.e., gift cards that were not cloned) at Company A stores. The defendant and his co-conspirators then returned the merchandise at Company A stores in exchange for clean gift cards.

9. During and in furtherance of the conspiracy, the defendant sold the clean gift cards for a profit. The defendant operated a business called “Capital Gift Cards,” with a website, which he used to sell clean Company A gift cards.

10. During and in furtherance of the conspiracy, the defendant personally engaged in dozens of—well more than a hundred—transactions using cloned gift cards at Company A stores. The defendant engaged in such transactions in numerous states, including Maryland, Virginia, the District of Colombia, Pennsylvania, Florida, Nevada, California, Delaware, New Jersey, and Connecticut. The defendant engaged in some of these fraudulent transactions in the Eastern District of Virginia.

11. As one example, on or about January 24, 2015, the defendant used a cloned gift card to purchase \$491.34 worth of merchandise at a Company A store in Sterling, Virginia, which is in the Eastern District of Virginia. The defendant’s purchases included one pair of shoes, two clean \$100.00 gift cards, and two clean \$125.00 gift cards. To purchase these items, the defendant used a cloned card with an encoded account number ending in -2964. The defendant’s use of the

gift card to make these purchases caused a wire transmission to be sent from Sterling, Virginia, to Company B in Florida and then to the Company A system in Ohio.

12. Subsequently, on or about February 3, 2015, Company A received a customer complaint regarding missing funds on the preexisting, legitimate gift card with the account number ending in -2964. The customer stated that the purchases made on January 24, 2015, in Sterling, Virginia, were not authorized. Company A subsequently reimbursed the customer in the amount of \$491.34, suffering a loss as a result.

13. As another example, the defendant and another co-conspirator ("CC-1") traveled to Las Vegas, Nevada, in or around April 2015. On or about April 24, 2015, the defendant and CC-1 conducted fraudulent transactions with more than 25 cloned gift cards in multiple Company A stores in or around Las Vegas. Throughout the day, the defendant and CC-1 communicated over text messages to coordinate the scheme. At one point, the defendant sent CC-1 a text message stating, "Imma try and go behind u too. This is a joke.!! We're gonna slaughter this town.!!" The total amount of the fraudulent transactions that the defendant and CC-1 engaged in that day exceeded \$13,500.

14. The defendant and CC-1 soon thereafter traveled to California, where they continued to carry out the fraudulent scheme. On or about April 26, 2015, the defendant and CC-1 used more than a dozen cloned gift cards in multiple Company A stores. The defendant and CC-1 coordinated their transactions over text messages. For example, at one point, the defendant asked CC-1, "Which register in [HomeGoods]?" CC-1 responded, "LITTLE OLD LADY FURTHEST FROM DOOR." CC-1 was encouraging the defendant to conduct a fraudulent transaction with the woman operating that register. The fraudulent transactions that the defendant and CC-1 engaged in that day totaled more than \$6,500.

15. Throughout and in furtherance of the conspiracy, the defendant also coordinated with Gray via cellphone in coded language to carry out the fraudulent scheme. On multiple occasions, Gray warned the defendant, in coded language, about efforts by Company A to investigate the scheme and identify the co-conspirators. For example, on or about December 16, 2014, Gray sent the defendant a text message stating, “Word is, images are being collected f[rom] MD area. Trying to identify the members of the book club.” Gray was warning the defendant, using code, that investigators were reviewing surveillance images from Company A stores in Maryland to try to identify the members of the conspiracy.

16. On or about April 30, 2015, the Montgomery County Police Department (“MCPD”) executed a state search warrant at the defendant’s residence at the Oxford House in Rockville, Maryland. The MCPD seized, among other things, a magnetic card encoder/reader, multiple gift cards, including more than 75 cloned Company A gift cards, and receipts that matched purchases that Hash and CC-1 made with cloned Company A gift cards.

17. Even after the execution of the April 30, 2015 search warrant, the fraudulent scheme continued and the defendant remained an active participant in it. The defendant, in fact, did not tell Gray about the search warrant for several months. In June 2015 alone, the defendant personally engaged in more than a dozen fraudulent transactions with cloned gift cards at Company A stores in the District of Columbia, Delaware, New Jersey, and Pennsylvania.

18. On September 2, 2015, the United States Secret Service (“USSS”) and MCPD executed a federal search warrant at the defendant’s residence in Bethesda, Maryland. The defendant was found in the rear bedroom pushing items into a hole in the wall. Law enforcement officers seized, among other things, 150 Company A gift cards, 36 of which were cloned.

19. The same day, on September 2, 2015, the USSS and Prince William County Police Department executed a federal search warrant at Gray's residence in Dale City, Virginia.

20. During and in furtherance of the conspiracy, the defendant and his co-conspirators engaged in hundreds of transactions using cloned gift cards at Company A stores across the nation. For each of these transactions, the cardholder who legitimately owned the account number that was charged did not authorize the defendant and his co-conspirators to use it. In total, the defendant caused a loss of approximately \$149,611.62 to Company A and its customers.

21. This statement of facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact known to the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

22. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

Respectfully submitted,


G. Zachary Terwilliger
United States Attorney

Date: August 1, 2019

By: _____

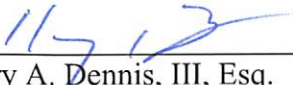

Thomas W. Traxler
Assistant United States Attorney

After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, MATTHEW HASH, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.



Matthew Hash
Defendant

I am Harry A. Dennis, III, the defendant's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.



Harry A. Dennis, III, Esq.
Attorney for Matthew Hash